

AMENDMENTS TO THE CLAIMS

This Listing of Claims will replace all prior versions, and listings, of Claims in the Application:

Listing of Claims:

Claim 1 (Currently Amended): An end to end real-time encrypting module of a mobile commerce WAP data transmission section, wherein the uppermost layer of the wireless application environment (WAE) is used as a developing platform and executing environment and is suitable for various communication networks, ~~such as~~ comprising at least one of GSM, PDC, CDPD, CDMA, TDMA, PHS, DECT, or GPRS and third generation mobile phone (3G); the real-time encrypting module comprising:

an information encryption code security system matching the public key infrastructure is being installed in a WML server end of a current mobile server of a wireless service provider; and the system includes a handset software encryption and decryption module, a cipher server, and a key management, said key management randomly generating an ideal key, said ideal key being stored and held secretly, said key management further generating a second set of keys which are in high demand and are frequently updated by a pseudo-random process, said key management further performing a secret sharing process wherein an original key is divided into a plurality of key shadows, said original key being restored only when a selected number of key

shadows are combined, said original key being non-recoverable when said original key is lost or destroyed; and,

a pre-compressor for compression of transmission data, said pre-compressor performing the pre-compression processing steps including:

a) dividing original data into a plurality of unit character strings, each said character string having 8 or 9 characters;

b) converting each said unit character string into a decimal value;

c) converting each said decimal value into a unit character string of hexadecimal characters;

d) dividing each said hexadecimal character into two unit character sets;

e) converting each said unit character set into a decimal character code between 0 and 255; and,

f) converting each said character code into a respective ANSI character set.

Claim 2 (Currently Amended): The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when an user registers into the WML server of WCP through a WAP network, the WML server will inform the cipher server to be responsible for actuating a public key remained in the handset software encryption and decryption module and the key management through the

cipher server for the inter-process communication interface provided by operation systems of various computers; the public key is downloaded to the client, ~~such as~~ comprising at least one of a mobile phone or a personal digital assistant, using HTTP service through a WAP gateway of WAN (wide area network), GSM/ GPRS/ CDMA and other digital mobile system.

Claim 3 (Currently Amended): The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when it is desired to down-link a personal commercial information, a user inputs a private key to be left in the stack memory of the mobile WAE environment as a standby key, further when the WML server transfers the personal commercial information to be down-linked to the cipher server, the WML server informs ~~and inform~~ the cipher server to open the public key ~~remained~~ remaining in the handset software encryption and decryption module and key management for executing an encryption algorithm in the server end in advance; ~~then~~ further, the handset software encryption and decryption module and the encrypted data are down-linked to a client through the HTTP service; then, the private key ~~remained~~ remaining in the WAE executing environment is used to decrypt the encryption data and then the decryption plain text is transferred to display the original form through a WML format document ~~for performing the following process.~~

Claims 4-6 (Canceled).

Claim 7 (Currently Amended): The end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein in the security mechanism, the handset software encryption and decryption module ~~is~~ are based on the WAE application layer, and thus ~~it is~~ are used to interpret wireless markup language, and wireless markup script language.